

## Cortafuegos de Windows Live OneCare: Una aproximación rápida a un problema duradero

### Introducción

A partir de junio, fecha en que **Microsoft** lanzó su conjunto de herramientas de seguridad **Windows Live OneCare**, se han sucedido una serie de discusiones respecto de cuánto y cómo, el producto beneficiaría a usuarios de ordenadores personales y si, realmente, brindaría la protección deseada, de forma confiable y fácil de utilizar.

A estas discusiones se sumaron las acusaciones (<http://sunbeltblog.blogspot.com/2006/06/microsoft-practices-predatory-pricing.html>) respecto de que **Microsoft** utilizaba políticas de precios depredadoras para eliminar la competencia y ponerle freno a la innovación en lo referido a seguridad informática para usuarios finales.

Para entender todos los ángulos de la discusión, decidimos adelantarnos, e instalar el producto, llevando a cabo nuestra evaluación respecto de la protección del programa cortafuegos de *OneCare*. Nos complace compartir los resultados de dicha evaluación en esta sección mensual de seguridad informática.

### A primera vista

La interfaz de *OneCare* luce sofisticada y bien organizada; tiene una colorida ventana de información desde la cual puede accederse a la configuración y comandos del programa.

Está desarrollado utilizando la tecnología **.NET**, propiedad de **Microsoft**, y necesita la instalación del paquete correspondiente, antes de utilizarlo.

Como estábamos interesados principalmente en la aplicación cortafuegos, analizamos en primer término la pestaña correspondiente, disponible desde el menú de configuración general.

Lo que sigue es la descripción de nuestra experiencia y las impresiones recogidas producto de su utilización.

### Tratamiento que realiza el cortafuegos sobre los programas

Por defecto, el cortafuegos de *OneCare* está configurado para actuar, de forma automática sobre los programas, controlando el acceso al mismo de acuerdo a la política de comportamiento, creada y proporcionada por **Microsoft**. Los programas que tienen permiso de conexión a Internet, se incluyen en la mencionada política y el cortafuegos simplemente les permite conectarse sin restricciones.

El problema con esta política es que cubre un número muy limitado de aplicaciones, y por lo tanto, el usuario está respondiendo continuamente las notificaciones de otros programas absolutamente legítimos que procuran tener acceso a Internet. Por otra parte, no existe forma de saber si el cortafuegos se encuentra en modo de acceso automático o definido por el usuario, ya que el primer modo bloquea el uso del acceso del programa a Internet y en seguida pregunta si debiese permitirse en situaciones futuras.

Lo que esto significa que, si un programa legítimo solicita acceso a Internet por primera vez, en nuestro caso el programa de conversación **IM (Chat)**, y no puede conectarse, después de un breve retraso, aparece en pantalla un mensaje al respecto. No es realmente una característica de la "facilidad de uso" el negar la conexión a Internet a los programas que intentan tener acceso por primera vez, y limita la funcionalidad del programa hasta un reinicio que restaure sus valores normales.

Los programas desconocidos son controlados por el cortafuegos de forma tal que les deja, a los usuarios, la impresión que cada programa es un potencial culpable - al ser bloqueado - hasta tanto se demuestre lo contrario.

No podemos decir lo mismo de cómo *OneCare* enfrenta las pruebas de fuga (*Leaktest*) (<http://www.firewallleaktester.com/>, <http://www.pcfank.com/>). Después de haberle permitido trabajar durante un par de horas, creando una base de datos de un tamaño razonable, con reglas de acceso a los programas, sometimos al programa cortafuegos a una selección de pruebas de fuga para verificar, de qué forma, el programa protegería a sus usuarios, de hipotéticos programas maliciosos que intentarían subir datos a la red desde el ordenador.

Los resultados fueron muy pobres, ya que el cortafuegos de *OneCare* pasó solamente las pruebas de fuga más básicas y simples, fallando en el resto. Resulta gracioso, pero considero a estas aplicaciones de prueba como que se trataba de programas como el Explorador de Windows, el navegador **Internet Explorer** u otros programas confiables, ampliamente utilizados en un ordenador basado en tecnología **Windows**, no pudiendo detectar, la tendencia de estas pruebas, a imitar, a inyectar código, o a secuestrar un programa confiable a nombre de quien obtener posteriormente las credenciales de acceso.

Las implicancias de este pobre resultado, son de gran envergadura: cualquier programa malicioso competente, no tendría ningún inconveniente para robar datos de un ordenador “protegido” por *OneCare*, mientras que el programa cortafuegos no emite ni una sola señal para evitar que esto suceda.

Se trata de un serio defecto, puesto que una de las principales funciones de una aplicación cortafuegos es la protección contra la conexión de programas no autorizados –tanto entrantes como salientes; en consecuencia, *OneCare* no resuelve los requisitos mínimos de una aplicación cortafuegos eficaz.

El programa cortafuegos es tan básico que incluso no estipula la creación de reglas avanzadas para el acceso de los programas, ya que sólo puede permitirse que un programa tenga acceso a Internet o lo tenga denegado.

No puede definirse una regla, que, por ejemplo, permita a la aplicación **Internet Explorer** tener acceso a algunos sitios Web y no a otros (tomando como base direcciones IP, por ejemplo).

Así como tampoco es posible especificar, por ejemplo, permisos de acceso temporal y aplicar a los programas parámetros avanzados de acceso a Internet, tales como la estipulación de puertos de acceso seguro y protocolos de acceso para un programa en particular. A pesar de estas importantes deficiencias, *OneCare* tiene otros aspectos, positivos y negativos, que vale la pena mencionar.

## Configuración de la red y prevención de la intromisión

La aplicación cortafuegos de *OneCare* detecta su configuración de red y puede limitar el acceso, de otros miembros de la misma red, a sus archivos e impresoras de usuario (una subred), estando restringido el acceso a Internet.

Con sólo otorgarle a los programas acceso a Internet, algo que resulta básico, dejan de poder crearse reglas avanzadas o especificar configuraciones avanzadas de “listas blancas” y “listas negras” de ubicaciones remotas o hacer más complejo el acceso al dominio de la red. Las mismas limitaciones de acceso se aplican a un escritorio remoto.

En forma sorprendente, *OneCare* carece de los estándares aceptados en la industria de los sistemas de seguridad informática respecto de intromisión, detección y protección, utilizados por la mayoría de las aplicaciones cortafuegos de terceros (**Outpost Firewall Pro**, **Norton Personal Firewall**).

Este es un serio descuido, ya que hoy se encuentran disponibles muchas herramientas utilizadas por piratas con las que se pueden generar en forma automatizada y a gran escala, intentos de intromisión, en millares de ordenadores personales, procurando encontrar aquellos que poseen una protección inadecuada, para ser aprovechados en el futuro. Estas herramientas son mejoradas y ampliadas constantemente, generando inconvenientes para los que **Microsoft** no proporciona ninguna clase de protección a los usuarios de su producto *OneCare*.

El paquete de filtros de *OneCare* está a la par de sus competidores, y la capacidad de seleccionar un rango de puertos para cualquier protocolo es una característica útil.

## Funcionamiento y compatibilidad

Aunque el programa funciona rápido en un ordenador de características medias, el tratamiento que da a los programas que se ejecutan por primera vez, es inaceptable.

Por defecto, todos los programas ejecutados, se someten a un análisis inicial de programas espía, efectuado por el programa **Windows Defender** de *OneCare* (actualmente en su versión beta 2), que retrasa la ejecución de la aplicación cerca de diez segundos.

Detectamos, hacia el final de nuestra evaluación, que esto no se puede limitar a la primera ejecución del programa ya que el programa **Windows Defender** se actualiza independientemente de la actualización del programa principal, y puede comenzar en cualquier momento, sin importar, por ejemplo, de cuánto ancho de banda se disponga. Si inicia, por ejemplo, cuando el usuario está en un punto clave en un juego en línea (aplicación de alta demanda), podría interrumpirlo.

También encontramos cuestiones relativas a la compatibilidad de *OneCare* aunque no las que podrían haberse esperado. Antes de instalar el programa, teníamos una aplicación cortafuegos ejecutándose en nuestro ordenador (como muchísimos usuarios). ¿Sospecha qué sucedió? El instalador de *OneCare* omitió advertirnos la necesidad de desinstalar el programa cortafuegos existente antes de realizar su propia instalación.

Así pues, descubrimos que *OneCare* se ejecutaba en paralelo a **Outpost Firewall Pro**, y que, este último, era el primero en supervisar el sistema, realizar preguntas y proteger al usuario, y no *OneCare*.

Antes de finalizar nuestra prueba, ocurrió otro incidente desafortunado: *OneCare* bloqueó el acceso conjunto a Internet de los navegadores instalados en nuestro ordenador (**Internet Explorer**, **Firefox**) permitiéndoles la conexión, sólo cuando la aplicación cortafuegos se encontraba en modo ocioso (apagado). Fue aquí cuando nos alejamos de *OneCare* definitivamente y sin demora.

## Conclusión

Aunque el programa es muy intuitivo, agradable a la vista, y fácil de utilizar – lo que resulta bueno para un nivel de usuarios inexpertos – es funcionalmente un gran retroceso y no tan solo no resulta útil sino que puede tornarse peligroso, al dar una falsa sensación de seguridad.

El producto *OneCare* de **Microsoft** necesita una revisión seria antes de poder considerarlo como algo más que una interfaz de lujo, sin seguridad real por debajo de dicha cubierta.